Escuela Colombiana De Ingeniería
Julio Garavito

Daniel Esteban Vela Lopez

Laura Valentina Rodriguez Ortegon

Andres Felipe Montes Ortiz

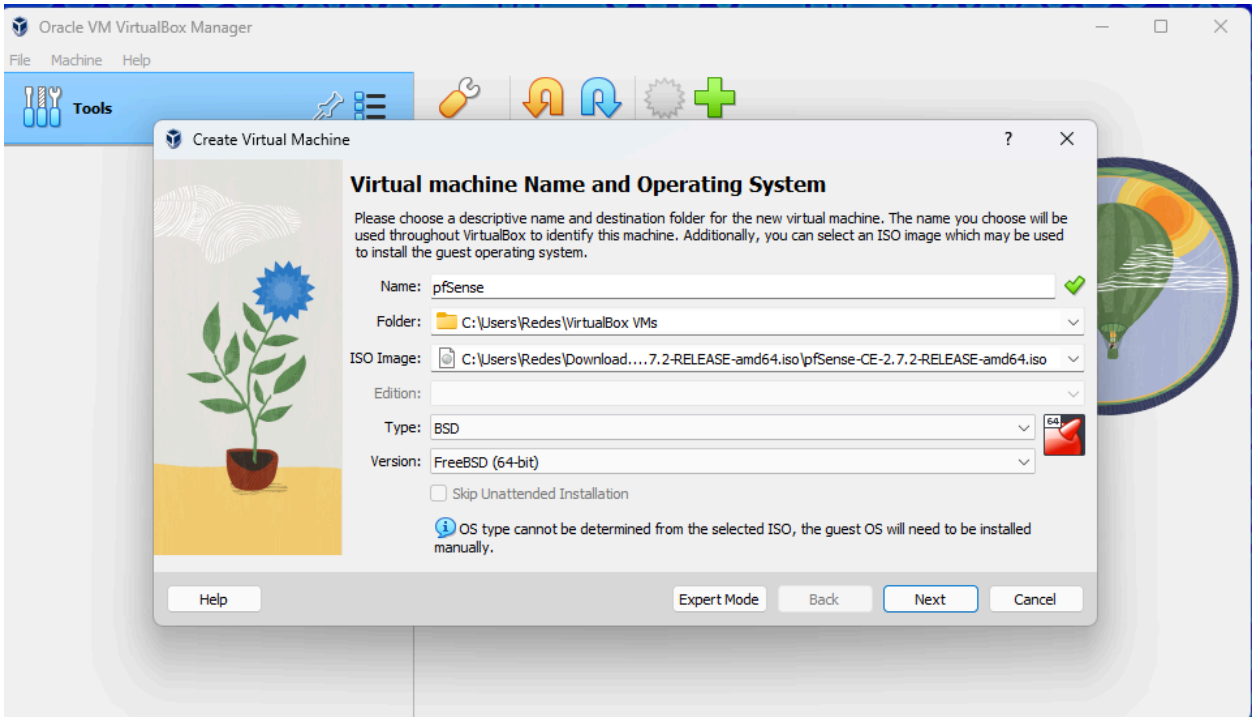
Laboratorio #15
2024-2

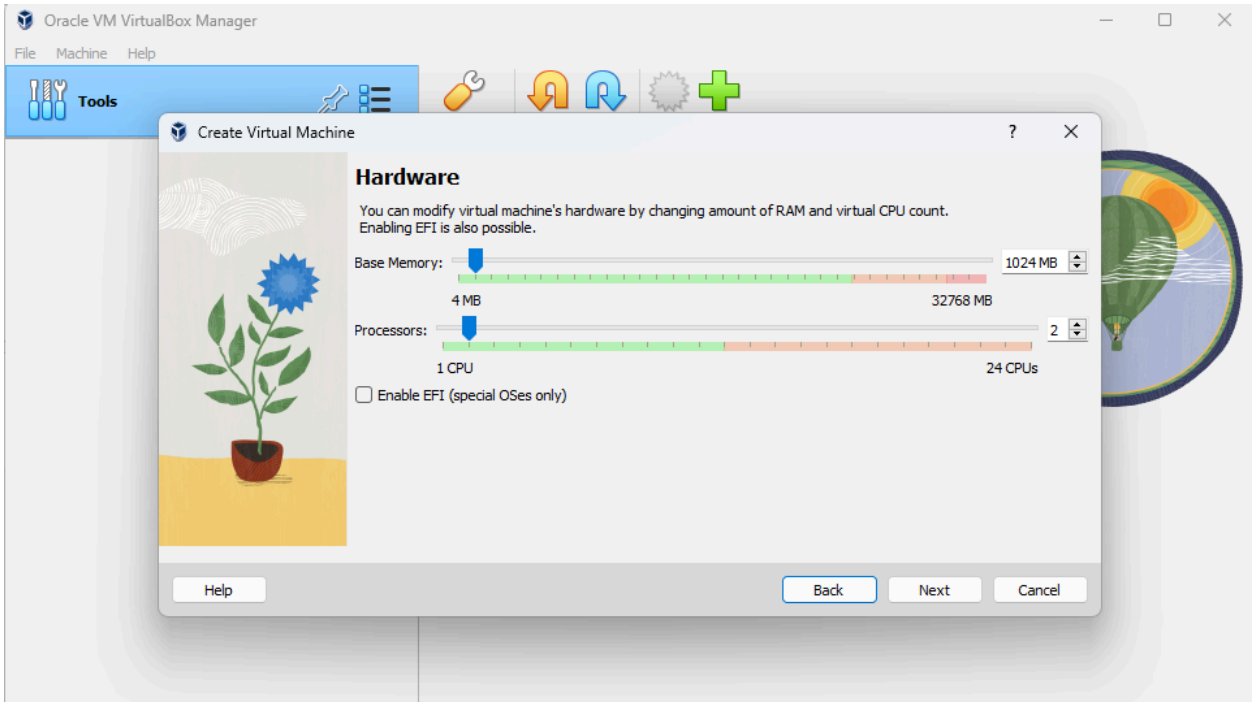
En este laboratorio, se instalará y configurará pfSense, un software de firewall, para restringir que la red 172.16.1.0/16 haga ping a la dirección IP externa 8.8.8.8. Primero, hay que asegurarse de que la máquina virtual pfSense (con dos interfaces de red) y las máquinas Kali estén en ejecución. Acceder a la interfaz web de pfSense desde Kali usando IP LAN (172.16.1.1). Por último, se ajustan las reglas del firewall para bloquear las solicitudes ICMP (ping) a la IP especificada.

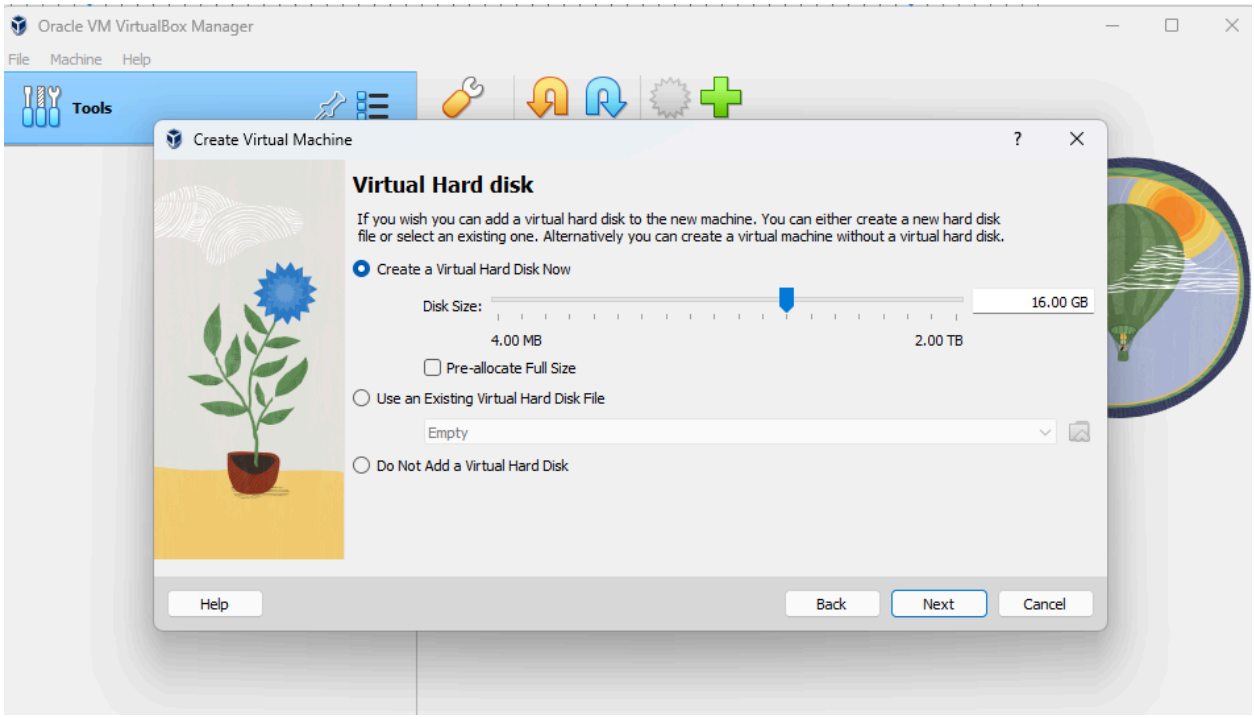
Primero, vamos a crear una nueva máquina virtual en VirtualBox.

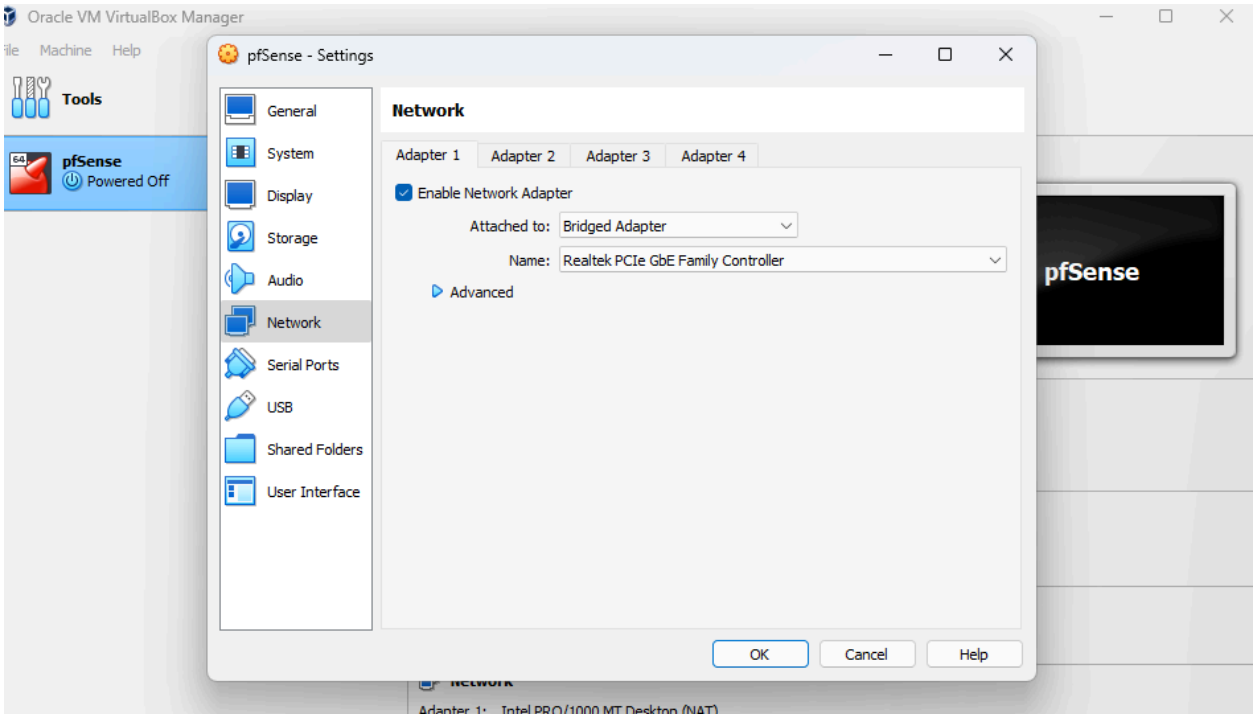
Seleccionamos la ISO de pfSense: Las instrucciones para instalar nuestro firewall. La descargamos de la página oficial de pfSense.

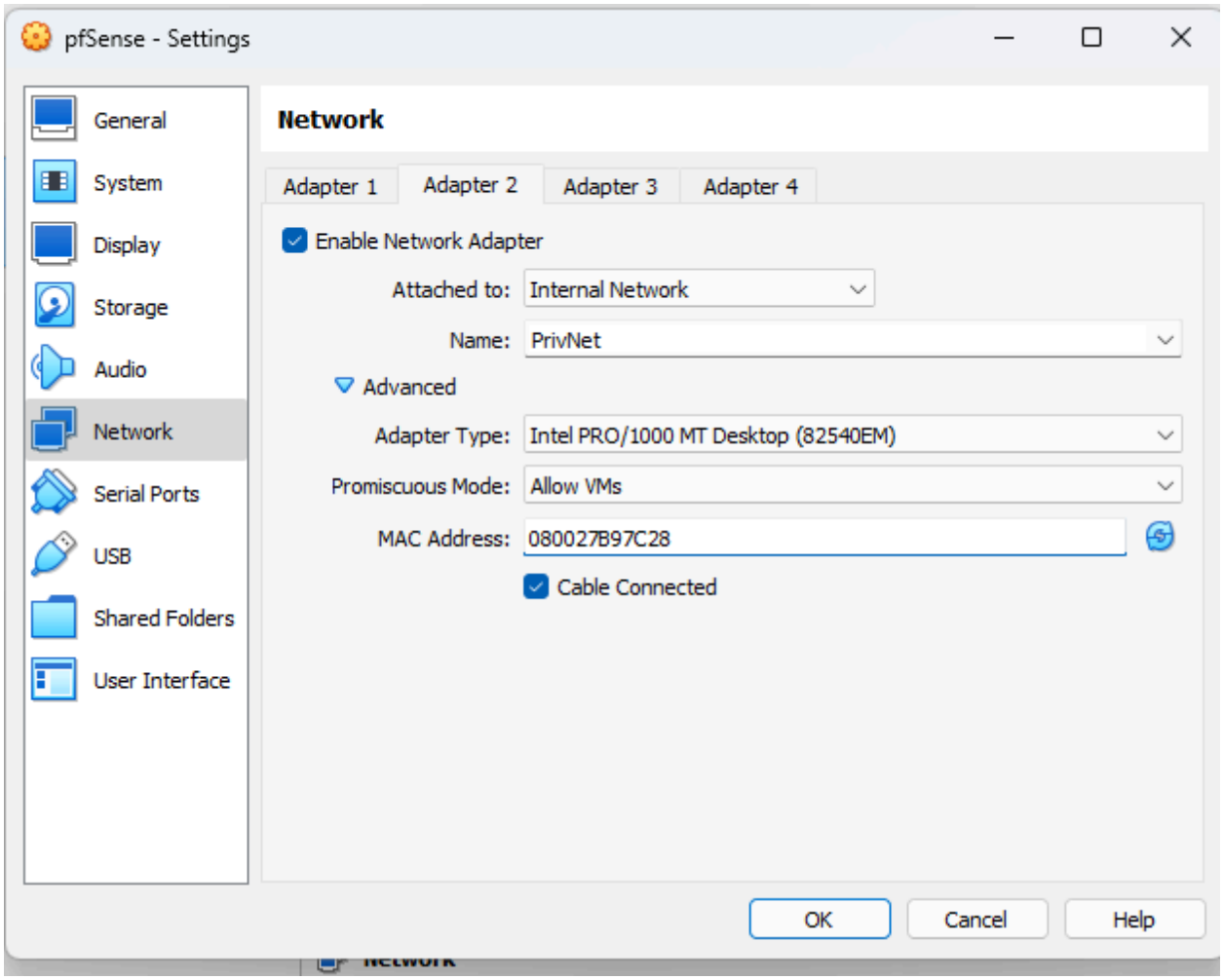
- ☐ **Le damos los recursos necesarios:**
  - **Memoria (RAM):** 1024 MB.
  - **Disco Duro:** 16 GB.
- ☐ **Configuramos las redes:**
  - **Adaptador 1 (Puenteado):** Este adaptador conectará nuestra máquina virtual directamente a nuestra red real.
  - **Adaptador 2 (Red interna "PrivNet"):** Crearemos una red interna para conectar otros dispositivos virtuales.



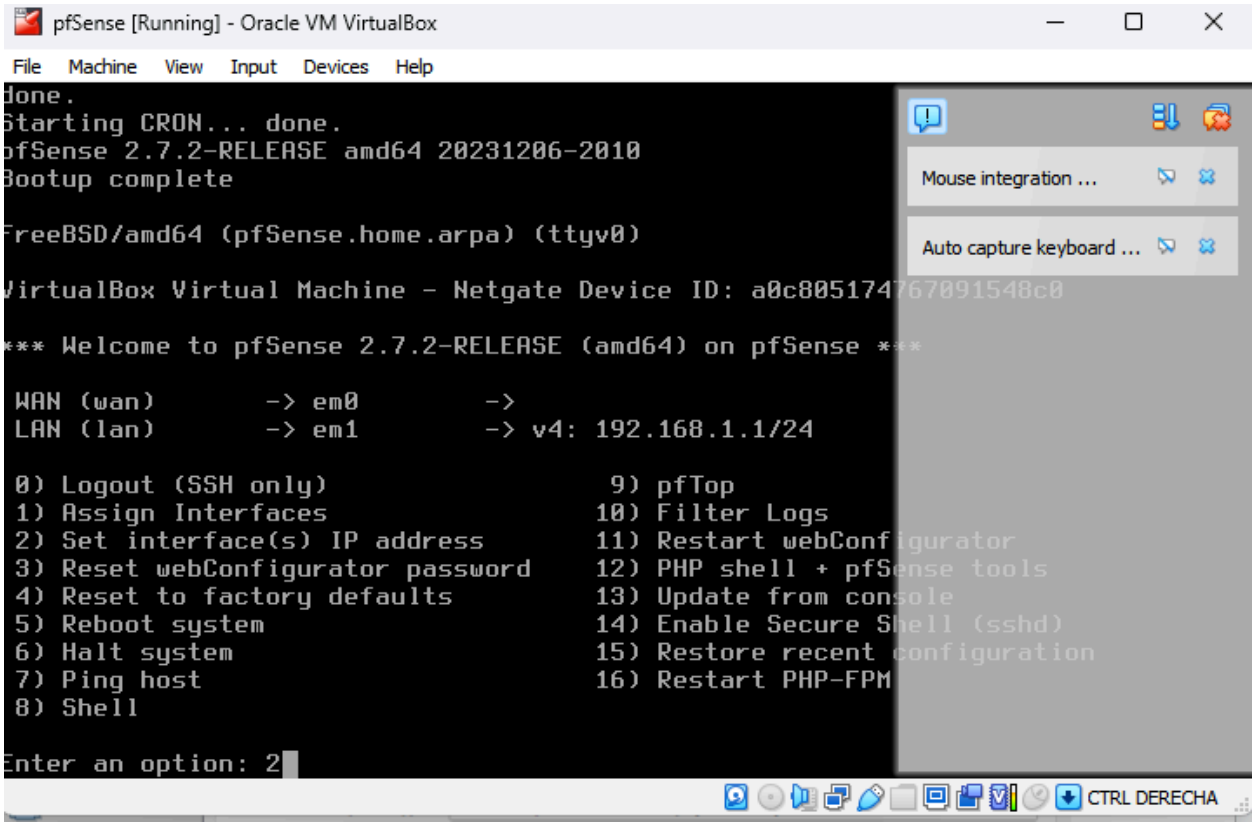

Oracle VM VirtualBox Manager
File
Machine
Help
Tools
Create Virtual Machine
Hardware
You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count.
Enabling EFI is also possible.
Base Memory:
1024 MB
4 MB
32768 MB
Processors:
2
1 CPU
24 CPUs
Enable EFI (special OSes only)
Help
Back
Next
Cancel


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
Create Virtual Machine
Virtual Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk
file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.
Create a Virtual Hard Disk Now
Disk Size:
16.00 GB
4.00 MB
2.00 TB
Pre-allocate Full Size
Use an Existing Virtual Hard Disk File
Empty
Do Not Add a Virtual Hard Disk
Help
Back
Next
Cancel


Oracle VM VirtualBox Manager
File Machine Help
Tools
pfSense
Powered Off
pfSense - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Bridged Adapter
Name:
Realtek PCIe GbE Family Controller
Advanced
OK
Cancel
Help
pfSense



Iniciamos nuestra máquina:



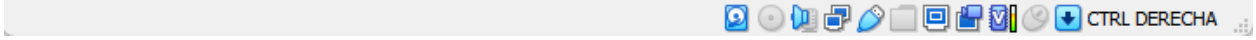
Lo primero que hicimos fue confirmar que queríamos configurar la interfaz número 2, que es justamente nuestra red interna "PrivNet". Luego, decidimos asignarle una dirección IP fija, en lugar de que la obtenga automáticamente. Elegimos la dirección 172.16.1.1, que será como la "dirección postal" de nuestra interfaz.

Después, definimos el tamaño de la red a la que pertenece esta dirección IP. Para eso, utilizamos una máscara de subred. Imagina que la red es una casa y la máscara de subred define el tamaño de cada habitación. En este caso, elegimos una máscara que nos permite tener una red de tamaño mediano.

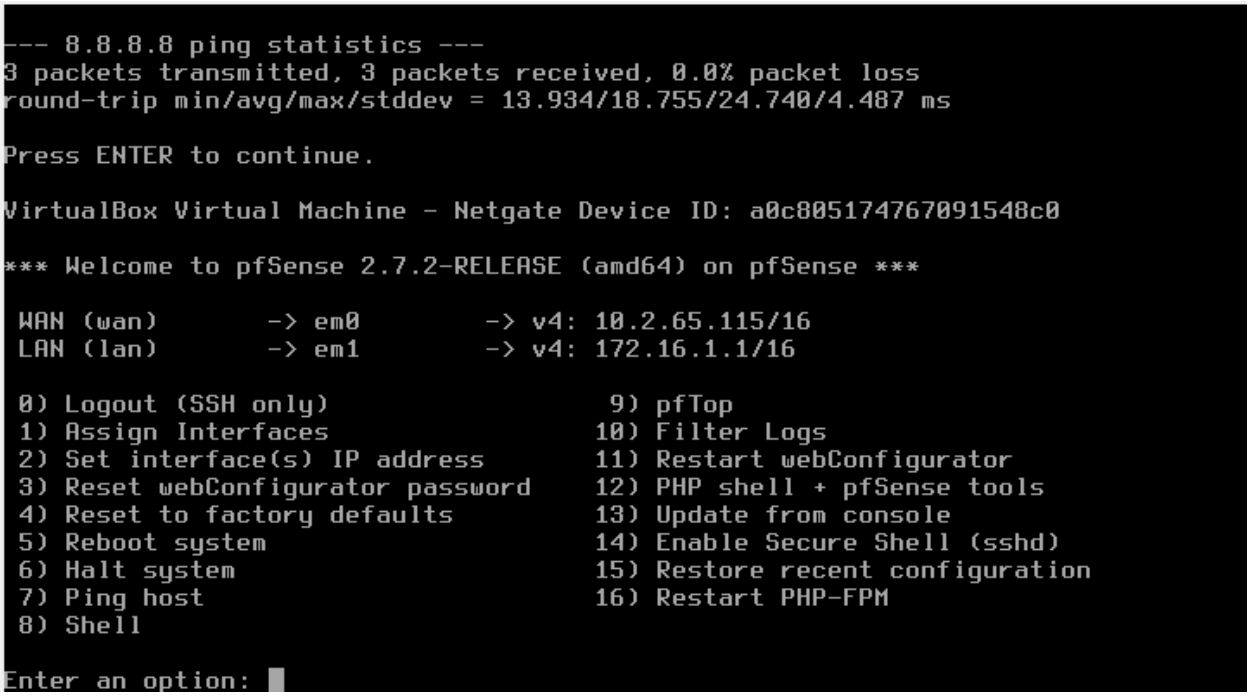
```
Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 172.16.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 16

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) nn

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>
```

Aquí asignamos un rango de IPv4 que podían ser utilizadas, desde 172.16.1.100 a 172.16.1.200

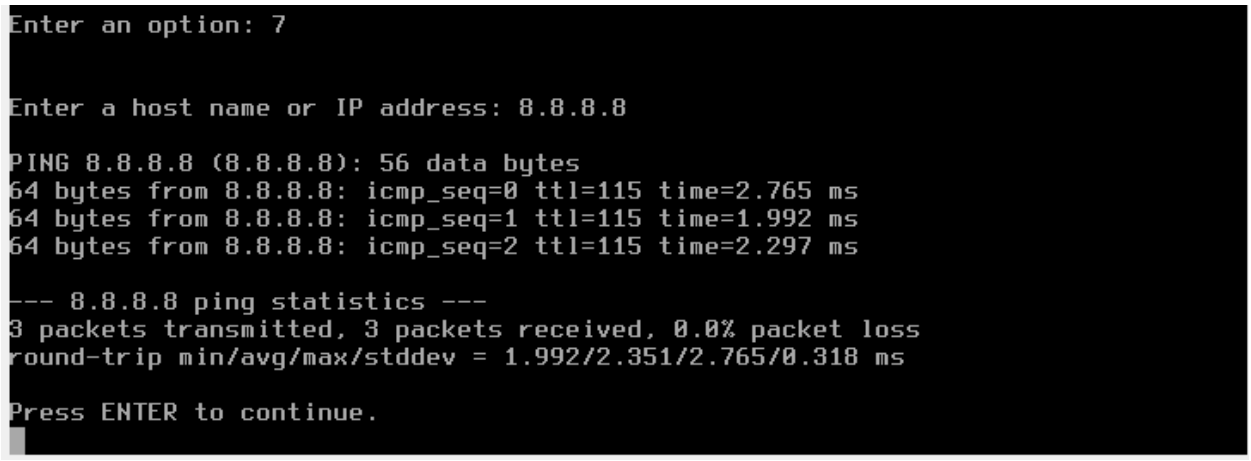
```
Configure IPv6 address LAN interface via DHCP6? (y/n) nn

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 172.16.1.100
Enter the end address of the IPv4 client address range: 172.16.1.200
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 172.16.1.1/16
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://172.16.1.1/

Press <ENTER> to continue.
```



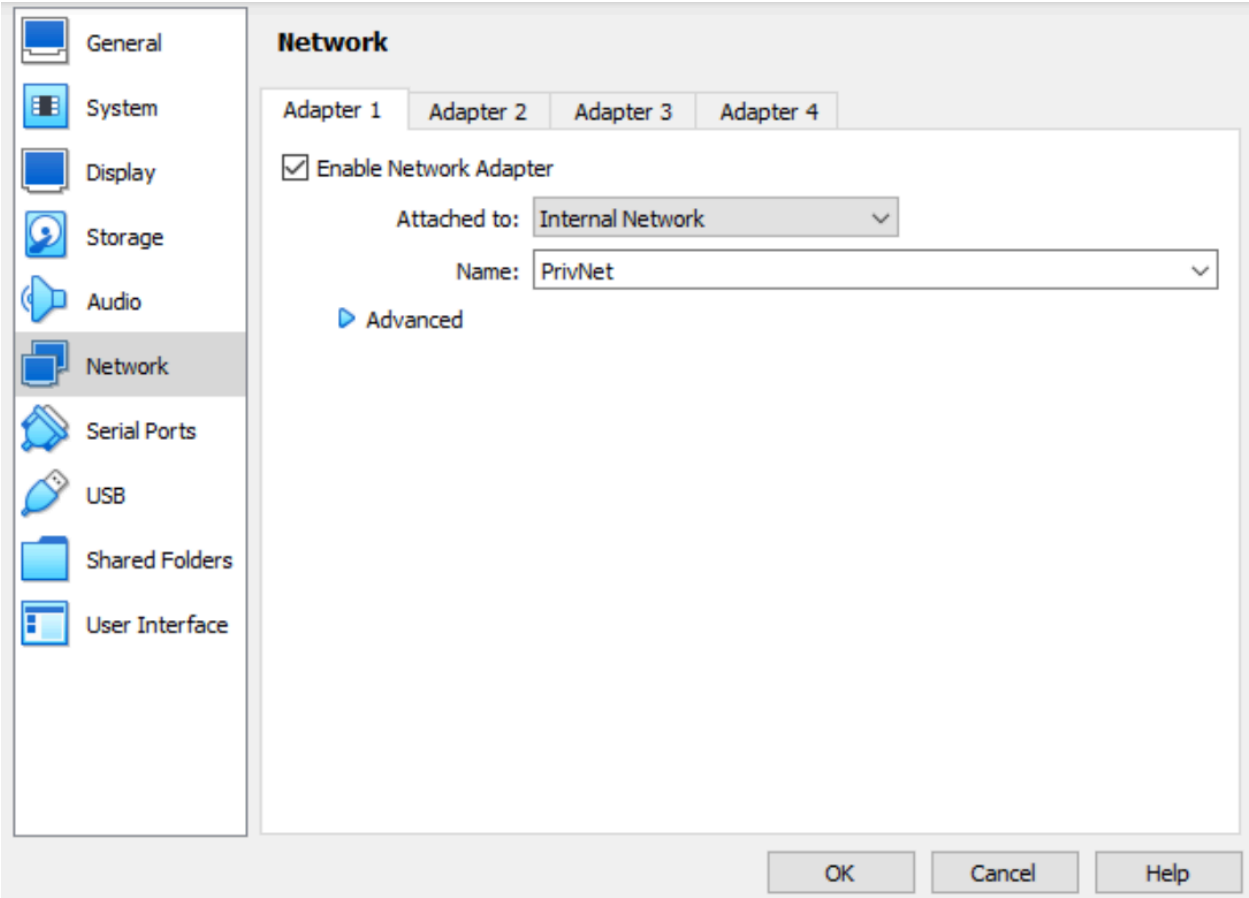
Acá está nuestra configuración final para nuestra WAN y LAN



Comprobamos que se haga ping en Google 8.8.8.8



Ahora vamos a verificar el servidor DHCP
Configuramos nuestro Network con una red privada

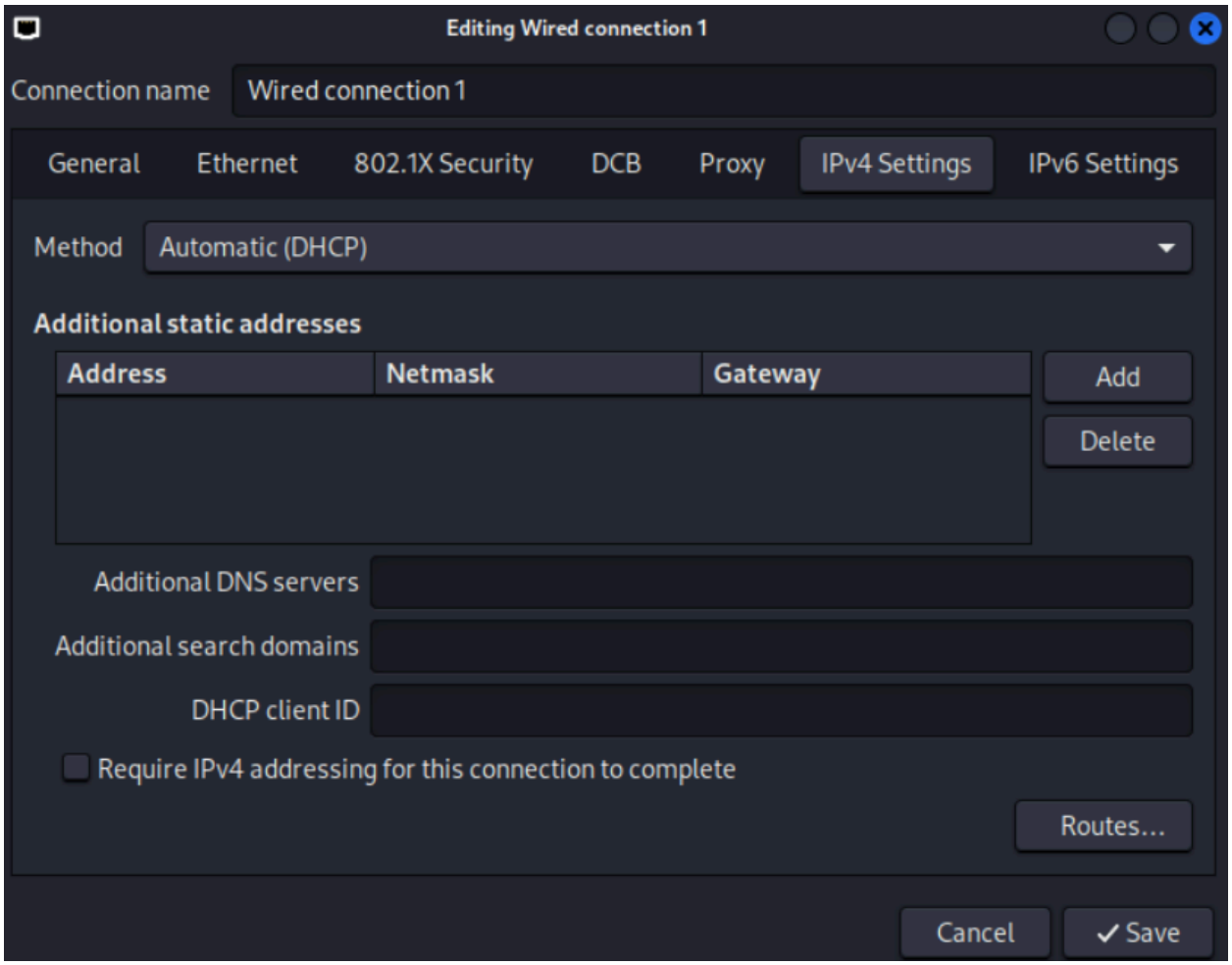


Una vez iniciada la máquina Kali Linux, verificamos la configuración de la interfaz de red 'PrivNet' ejecutando un ping hacia la dirección IP de pfSense. Si la prueba es exitosa, confirmamos que la comunicación entre ambas máquinas se ha establecido correctamente.

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.1.100  netmask 255.255.0.0  broadcast 172.16.255.255
        inet6 fe80::4e33:2ce:73f0:4bef  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 16  bytes 2810 (2.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 54  bytes 6747 (6.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

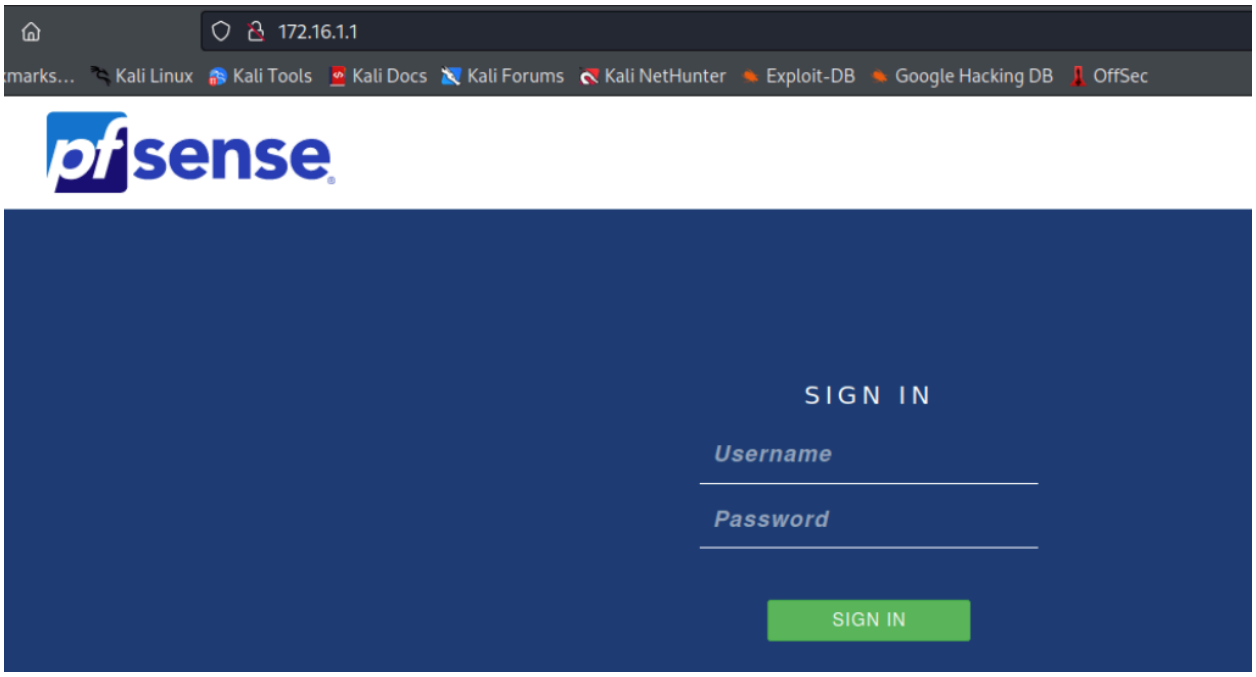
```
┌──(kali㉿kali)-[~]
└─$ ping 72.16.1.100
PING 72.16.1.100 (72.16.1.100) 56(84) bytes of data.
64 bytes from 72.16.1.100: icmp_seq=1 ttl=47 time=124 ms
64 bytes from 72.16.1.100: icmp_seq=2 ttl=47 time=127 ms
64 bytes from 72.16.1.100: icmp_seq=3 ttl=47 time=114 ms
64 bytes from 72.16.1.100: icmp_seq=4 ttl=47 time=122 ms
```

Accedemos a la configuración de red del sistema operativo y seleccionamos la conexión por cable (Wired connection 1). A continuación, configuramos la obtención automática de la dirección IPv4. Para verificar la correcta configuración, ejecutamos un comando ping hacia el servidor DNS de Google (8.8.8.8) y comprobamos que se reciben respuestas.

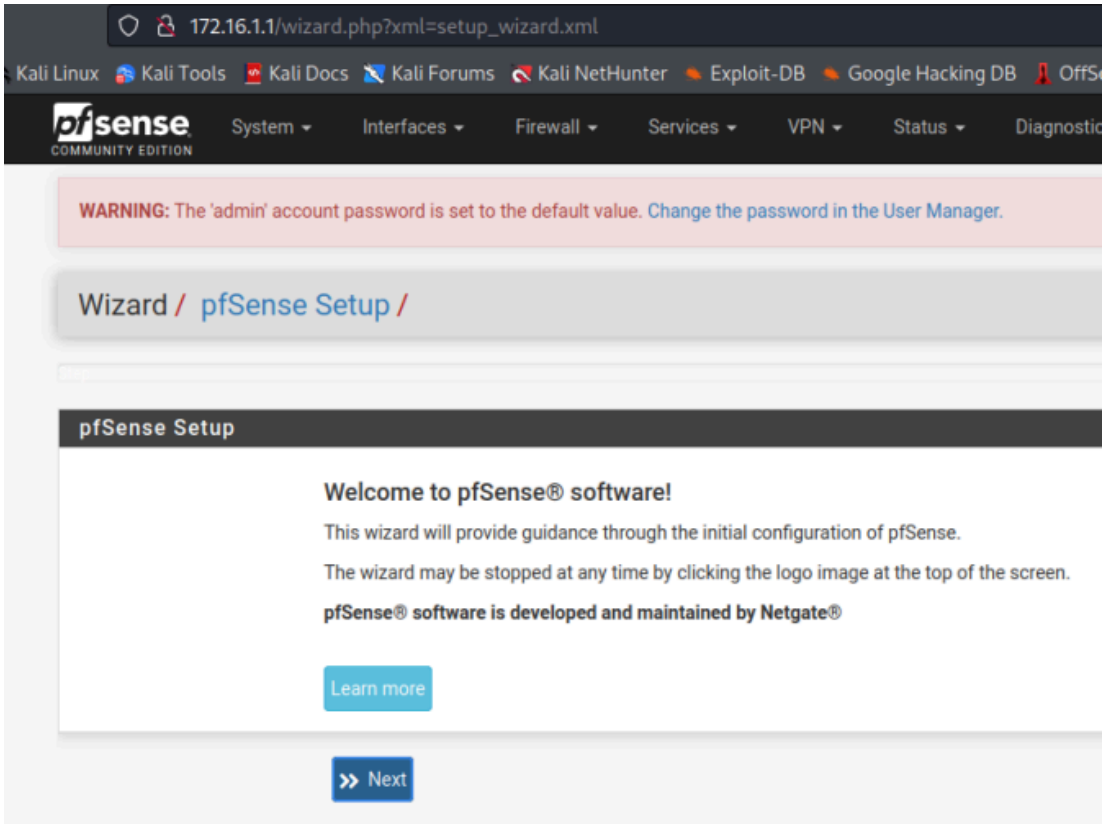


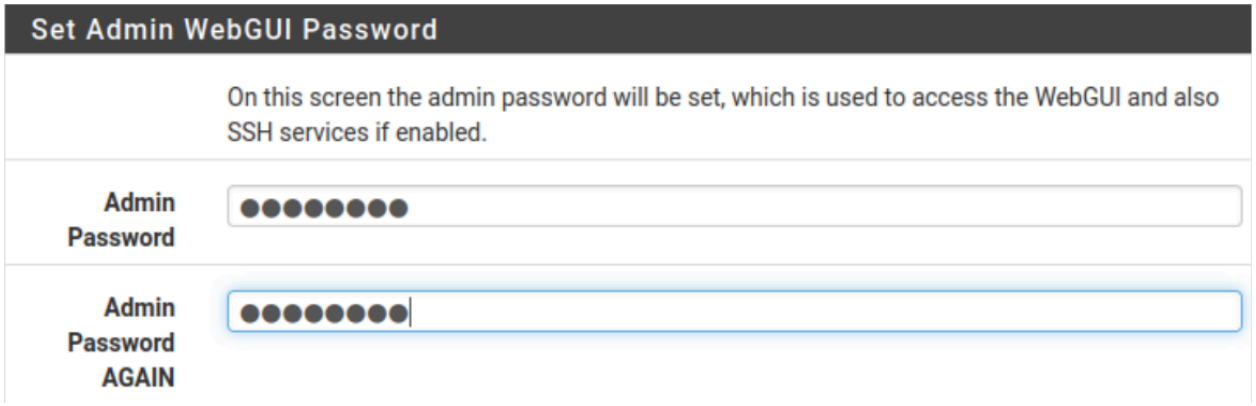
```
┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=3.55 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=4.30 ms
^Z
zsh: suspended  ping 8.8.8.8
```

Accedemos a un navegador web, e ingresamos en la barra de direcciones la dirección IP de la interfaz de red LAN de pfSense. Esta acción nos permitirá acceder a la interfaz web de administración del firewall.



Siguiendo las instrucciones del asistente de configuración, establecemos el servidor DNS primario como '8.8.8.8' y procedemos a modificar la contraseña de administrador, asignándole un valor seguro y complejo.





A continuación, accedemos a la sección de reglas de firewall y creamos una nueva regla. En esta regla, configuramos la acción como 'bloqueo', la interfaz como 'LAN' y establecemos como destino la dirección IP '8.8.8.8'. De esta manera, impediremos cualquier tipo de comunicación desde nuestra red local hacia el servidor DNS de Google.

Edit Firewall Rule

Action
Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled
☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface
LAN

Choose the interface from which packets must come to match this rule.

Address Family
IPv4

Select the Internet Protocol version this rule applies to.

Protocol
ICMP

Choose which IP protocol this rule should match.

ICMP Subtypes
any
Alternate Host
Datagram conversion error
Echo reply

For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Destination

Destination
☐ Invert match
Address or Alias
8.8.8.8 /

Extra Options

Log
☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

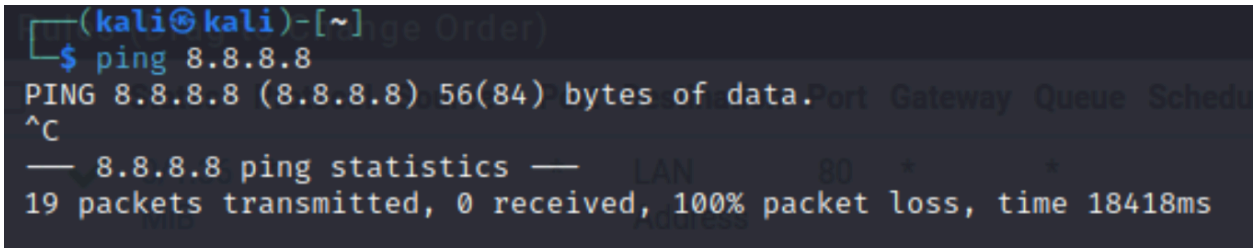
Description
No more ping to Google's DNS

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options
Display Advanced

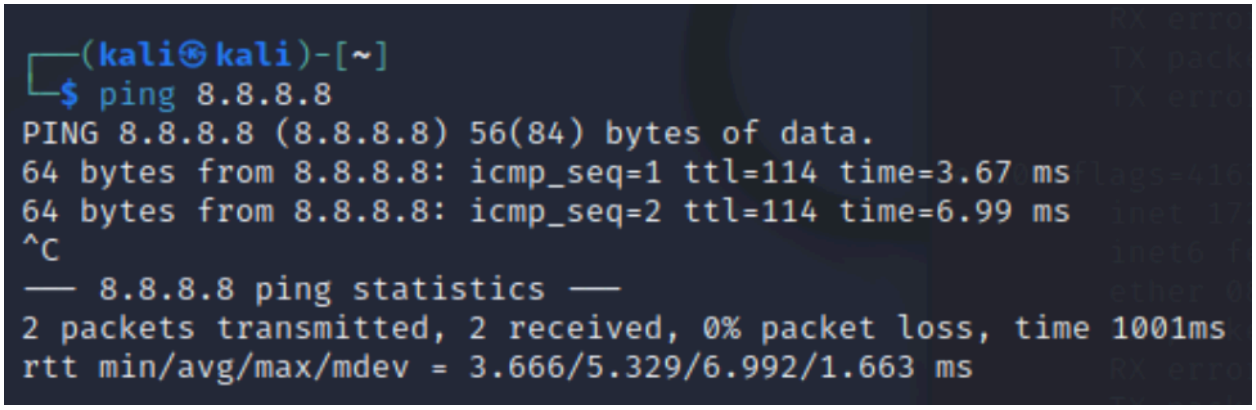
Save

Si nos vamos a nuestra consola, veremos que no es posible la conexión y si cambiamos la conexión, estará activa nuevamente.



Así se verá nuestra configuración cuando no esté permitida:

Y la configuración cuando si está disponible se verá:



Con la configuración realizada, pfSense actúa como un router, asignando direcciones IP a los dispositivos de la red a través de su servidor DHCP, y como un firewall, filtrando el tráfico de red de manera granular. Además, hemos

implementado una política de seguridad que bloquea el acceso a servicios no esenciales, como el servidor DNS de Google, y permite el acceso remoto a través de una conexión VPN segura. De esta manera, garantizamos la protección de nuestra red y la privacidad de los datos.